AMENDMENTS TO THE CLAIMS

Please amend Claims 1, 5, 7, and 8, cancel Claims 6 and 9, and add new Claims 10-20.

1. (Currently Amended) A method of transferring ~~files~~ data over a computer network from a network server to a client computer system, the method comprising:

receiving a request by a requestor using a client computer system for data from at [[a]]least one network server ~~from a client computer system~~;

checking [[a]] ~~file~~ an attribute of the requested data ~~using the network server~~ to determine whether the requested data is encrypted with an encryption key;

if the requested data is encrypted with the encryption key, checking the attribute of the requested data to determine an owner of the encryption key; and

comparing the owner of the encryption key obtained from the attribute with the requestor to determine whether the requestor is the owner of the encryption key

~~automatically retrieving using the network server a public encryption key from said client computer system when the data is not encrypted;~~

~~encrypting the unencrypted data with said public encryption key automatically and without user intervention; and~~

~~sending the encrypted data to said client computer system~~.

2.-4. (Canceled)

5. (Currently Amended) A method of data storage and retrieval comprising:

automatically generating independently of information from a network server a public encryption key and a corresponding private encryption key in a client computer system;

storing ~~said~~ the public encryption key and ~~said~~ the corresponding private encryption key in ~~said~~ the client computer system;

associating an attribute with a data file, the attribute indicating whether the data file is encrypted with the public encryption key when stored on the network server, and the attribute indicating an owner of the public encryption key;

requesting the[[an]] ~~unencrypted~~ data file by a requestor from the network server using ~~said~~ the client computer system;

checking the attribute of the requested data file to determine whether the requested data file is encrypted;

if the requested data file is encrypted, checking the attribute of the requested data file to determine an owner of the public encryption key;

comparing the owner of the public encryption key obtained with the attribute with the requestor to determine whether the requestor is the owner of the public encryption key

~~sending said public encryption key from said client computer system to said network server automatically and without user intervention, wherein said public encryption key is used to encrypt said unencrypted data file to create an encrypted data file;~~

~~receiving said encrypted data file at said client computer system; and~~

~~storing said encrypted data file on a storage medium in said client computer system~~.

6. (Canceled)

7. (Currently Amended) The method of Claim 5, wherein ~~said~~ the public encryption key and ~~said~~ the corresponding private encryption key are based on a password entered by a user when logging on to ~~said~~ the client computer system.

8. (Currently Amended) A computer readable data storage medium having stored thereon commands that are operative to cause a general purpose computer configured as a network server to perform a method of data retrieval comprising ~~the steps of~~:

receiving a request from a requestor for a data file from a client computer system;

checking a file attribute of the requested data file to determine whether the requested data file is encrypted with an encryption key;

if the requested data file is encrypted with the encryption key, checking the file attribute of the requested data file to determine an owner of the encryption key; and

comparing the owner of the encryption key obtained from the attribute with the requestor to determine whether the requestor is the owner of the encryption key

~~based at least in part on the attribute, automatically requesting a public key from said client computer system, the public key being originated independently of the network server;~~

~~automatically encrypting said data file using said public key; and~~

~~routing said encrypted data to said client computer system~~.

9. (Canceled)

10. (New) The method of Claim 1, further comprising:

if the requested data is unencrypted, automatically retrieving the encryption key associated with the requestor from the client computer system;

encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data; and

sending the encrypted data to the client computer system.

11. (New) The method of Claim 1, further comprising sending the requestor a message indicating the requested data is not encrypted with the encryption key associated with the requestor if the requested data is encrypted and the requestor is not the owner of the encryption key.

12. (New) The method of Claim 1, further comprising sending the requested data to the client computer system if the requested data is encrypted and the requestor is the owner of the encryption key.

13. (New) The method of Claim 1, wherein the encryption key is derived at least in part from an identification code.

14. (New) The method of Claim 13, wherein the encryption key is derived at least in part from user input.

15. (New) The method of Claim 5, further comprising:

if the requested data file is unencrypted, sending the public encryption key from the client computer system to the network server automatically and without user intervention;

receiving the requested data file at the client computer system after the public encryption key is used to encrypt the requested data file to create an encrypted data file; and

storing the encrypted data file on a storage medium in the client computer system.

16. (New) The method of Claim 5, further comprising sending the requestor a message indicating the requested data file is not encrypted with the public encryption key associated with the requestor if the requested data file is encrypted and the requestor is not the owner of the public encryption key.

17. (New) The method of Claim 5, further comprising sending the requested data file to the client computer system if the requested data file is encrypted and the requestor is the owner of the public encryption key.

18. (New) The data storage medium of Claim 8, further comprising:

if the requested data file is unencrypted, automatically requesting the encryption key associated with the requestor from the client computer system, the encryption key being originated independently of a network server;

automatically encrypting the requested data file using the encryption key associated with the requestor to create an encrypted data file; and

routing the encrypted data file to the client computer system.

19. (New) The data storage medium of Claim 8, further comprising sending the requestor a message indicating the requested data file is not encrypted with the encryption key associated with the requestor if the requested data is encrypted and the requestor is not the owner of the encryption key.

20. (New) The data storage medium of Claim 8, further comprising sending the requested data file to the client computer system if the requested data file is encrypted and the requestor is the owner of the encryption key.